



# FedRAMP Online Training

## How to Write a Control

3/15/2016

**Presented by: FedRAMP PMO**



# Today's Training

- Welcome to Part Six of the FedRAMP Training Series:
  1. Introduction to the Federal Risk and Authorization Program (FedRAMP) – 100A
  2. FedRAMP System Security Plan (SSP) Required Documents – 200A
  3. FedRAMP Review and Approve (R&A) Process – 201A
  4. Security Assessment Plan (SAP) Overview – 200B
  5. Security Assessment Report (SAR) Overview – 200C
  - 6. How to Write to a Control – 101A**
  7. Continuous Monitoring Overview
- This course aims to assist CSPs in writing compliant control implementation descriptions in the SSP.



# Training Objectives

- At the conclusion of this training session you should understand:
  - Document acceptance criteria
  - Technical acceptance criteria
  - What is expected in a control implementation description
  - The difference between a good control implementation description and a poor control implementation description



# FedRAMP Mindset for SSP Development

1. Allocate Sufficient Time and Effort for Writing

2. Strongly and Clearly Articulate Security Architecture and Implementations

3. Tell a Story

4. Answer Who, What, When, Where, Why and How



5. Answer 100% of the Controls

6. Be Clear, Concise, Consistent, and Complete

7. Adequately Reference all Documentation

8. Ensure Compliance with FedRAMP Policy



# Basic Writing Tips

- Use the correct FedRAMP SSP template and do not modify or remove sections
- Use consistent terminology throughout the SSP
  - Refer to any system element or document cited in the text, in exactly the same way throughout the SSP, such as:
    - System name and system abbreviation
    - Hardware or software elements
    - Document cites, which must contain document title, version, and date
- Be direct and to the point - avoid run-on sentences and use of the passive voice
- After all descriptions are written, run grammar/spell check
- After all descriptions are written, also read through the control implementation descriptions to check for:
  - Errors not discovered by grammar/spell check
  - Checkboxes that have not been appropriately marked
- Every control part (Part a, Part b, Part c , etc.) should contain a focused discussion on the specific control requirement



# Document Acceptance Criteria

## Clear

- Material is unambiguous, clear, and comprehensive
- Written in correct and consistent format
- Logical presentation of material

## Concise

- Content and complexity are relevant to the audience
- No superfluous words or phrases
- Omit words that don't add meaning

## Consistent

- Terms have the same meaning throughout the document
- Items are referred to by the same name or description throughout the document
- The level of detail and presentation style are the same throughout the document

## Complete

- Responsive to all applicable FedRAMP requirements
- The Security Package Includes all appropriate sections of the FedRAMP template
- The Security Package Includes all attachments and appendices



# Technical Acceptance Criteria

## Readable

- Refers to the *Four Cs* for text – *Clear, Concise, Complete, and Consistent*
- Is there a clear understanding of what was written?

## Relevant

- Refers to the control implementation description addressing the specific control requirement(s) including any parameters
- Did the statement address the control requirement?

## Sufficient

- Refers to the detail and thoroughness contained in the control implementation description - it should be sufficient to allow a reader to understand what is done and **how** it is done
- Is there enough detail to fully address all portions of the requirement?

## Complete

- Refers both to the control implementation description's agreement with the marked control template checkboxes and its consistency with other SSP text
- Do the implementation statements and the control template checkboxes match?



# A Poor Control Implementation Description

- Repeats or rephrases the control requirement instead of describing how it is addressed in the system
- Uses “boilerplate” text copied and pasted over and over again
- Contains text not directly relevant to describing how the control is implemented
- Is left blank for example no control implementation description has been written
- Is marked N/A when it is not, or is marked N/A without a risk based justification of why it is considered N/A



# A Poor Control Implementation Description

- Inappropriately cites a document or does not contain sufficient detail to demonstrate that the control is implemented and compliant
- Does not identify all persons responsible (by role) for implementing/enforcing the solution to the security control
- Does not describe all possible places where a control is implemented
- Where a single control contains multiple requirements, does not address all requirements
- The wrong Implementation status is checked



# Readability Example

## AC-17, Part a

- Asks for establishment and documentation of usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed

- Poor Example – AC-17, Part a:

Remote access for privileged functions be permitted only for compelling operational needs, shall be strictly controlled, and must be approved in writing by <role named> . . . The number of users who can access <system name> remotely is limited and approval for such access is documented.

- The example above is difficult to read and understand because:
  - The text “meanders” around the point of what the control requires, is off-topic, and is non-specific; this makes it difficult for a reviewer to understand what was meant.
  - Insufficient because it does not address all of the specific requirements of the control.



# Relevancy Example

## CA-1

Requires:

- The policy is reviewed and updated [every three years] and
- The procedures are reviewed and updated [at least annually]

- Poor Example – CA-1, Part b

*Certification, authorization, and security assessment procedures address all areas in the policy and policy-compliant implementations of related security controls.*

- The example is not relevant because it does not address the specifics of CA-1, Part b; a better example might be:

*<System Name> certification, authorization, and security assessment policies are reviewed and updated by <role(s)> at least every three years using <describe process>; the associated procedures are reviewed and updated by <role(s)> at least annually using <describe process>.*



# Sufficiency Example

## CP-9 : Part c

- Requirements include backup of system documentation (daily incremental, weekly full), and at least three backup copies

- Poor Example – CP-9, Part c

The XYZ system has data backup procedures in accordance with control requirements. Daily incremental and weekly full backups are performed . . . *(sufficient technical details about which backup procedures are then provided in the control implementation description).*

- This example control implementation description is insufficient because it does not specifically mention backup of system documentation, and does not address the FedRAMP requirement for at least three backup copies at all.



# Case Study: Account Management (AC-2)

## The organization:

- a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: *[Assignment: organization-defined information system account types]*;
- b) Assigns account managers for information system accounts;
- c) Establishes conditions for group and role membership;
- d) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- e) Requires approvals by *[Assignment: organization-defined personnel or roles]* for requests to create information system accounts;
- f) Creates, enables, modifies, disables, and removes information system accounts in accordance with *[Assignment: organization-defined procedures or conditions]*;
- g) Monitors the use of information system accounts;
- h) Notifies account managers:
  - 1) When accounts are no longer required;
  - 2) When users are terminated or transferred; and
  - 3) When individual information system usage or need-to-know changes.
- i) Authorizes access to the information system based on:
  - 1) A valid access authorization;
  - 2) Intended system usage; and
  - 3) Other attributes as required by the organization or associated missions/business functions.
- j) Reviews accounts for compliance with account management requirements *[FedRAMP Assignment: at least annually]*; and
- k) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.



# Control Definition

Each control objective (a-k) must be answered individually.

- As a guide to understanding the requirements for each control, the Rev 4 Test Cases may be reviewed.

Use the control as a cascading point to the rest of the definition (ex: AC-2b)

- “The organization...” Assigns account managers for information system accounts.
- “The organization...” Establishes conditions for group and role membership.

Look at the verb in the control requirement: **Assigns**

- The verbs in each control explain the action to be implemented and must be used in the implementation description.

Here is where the story-telling begins:

- Who (from the identified roles) assigns account managers?
- How and when are account managers assigned? Tell us how this is done. What is the process? Who is informed? When? How are they informed? What records are kept?
- Walk the reader through it like writing a story (beginning, middle, and end)

## Keep in mind:

- ✓ If a 3PAO is going to verify/validate this control, is this implementation detailed enough for them to know what evidence/artifacts to request or what the logical next steps are?
- ✓ As a CSP, can I provide evidence for the 3PAO to examine or test, and can a CSP team member vouch for an implementation if interviewed?



# Control Writing Tips

## Organization Defined

- Organization-defined assignments must be defined and documented by a CSP
- Acceptable references may come from Standard Operating Procedures, Security Policy, or Concept of Operations guides

### Staying with AC-2, let's look at assessment objective (a):

Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];

- The control is asking the CSP to **identify** and **select** the types of information system accounts to support organizational missions/business functions
- The CSP can choose to include a reference to the policies where these accounts are identified, as long as the reference includes the **name**, **date**, and **version** of the policies, and the **section number** or **page number** where these accounts can be located



# Control Writing Tips

## FedRAMP Assignments

- These follow the same logic as organization-defined assignments and must be treated as such
- The assignments are also documented in the “Parameter” sections of the Control Summary Information following the requirements

### Requirements with multiple items (AC-2f)

The organization: **Creates, enables, modifies, disables, and removes** information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];

- Each action must be addressed individually with the same level of detail to satisfy the control, so that it is testable



## Information that Can Help You

- Use the FedRAMP website, [www.fedramp.gov](http://www.fedramp.gov), to:
  - Obtain the SSP template
  - Read “Tips and Cues”
  - Read the FedRAMP Newsletter
  - Access FedRAMP reference and training materials
- Reference NIST Special Publication 800-53, Revision 4, which contains supplemental guidance for each NIST control
- For questions about FedRAMP, email [info@fedramp.gov](mailto:info@fedramp.gov)



# FedRAMP

Federal Risk Authorization Management Program

*For more information, please contact us or visit us at any of the following websites:*

<http://FedRAMP.gov>

<http://gsa.gov/FedRAMP>

Follow us on  @FederalCloud